LISTING OF THE CLAIMS:

Claims 1-14 (Cancelled).

15. (Previously Presented) A computer system for reading in a password and generating an encrypted password in a secure manner, the computer system comprising:

a central processing unit (CPU);

a random access memory (RAM);

an input/output (I/O) interface including a password input device for receiving a user password from a user;

an operating system including a cryptographic-function generator module for creating program-specific identifiers and program-password-specific identifiers;

a password request program;

a password reading program;

an indicator means connected to the operating system to provide a signal indicating that the user password has been inputted;

wherein the operating system, the CPU, the RAM, and the I/O interface form a trusted computing base (TCB);

the password request program being connected to a commercial entity that that asks for entry of the user password, said commercial entity pre-storing a transformed password F [H(E), p];

the password request program receiving the inputted user password from the TCB;

PAGE 7/11 * RCVD AT 7/26/2005 2:26:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:5167424366 * DURATION (mm-ss):02-40

upon receiving a request from the entity for the transformed password, the password request program forwarding said request to the password reading program;

the generator module generating a program-specific identifier H(E) and a program-password specific identifier;

the password request program sending a message to the password reading program, said message including the program–specific identifier H(E);

in response to receiving said message, the password reading program locks the I/O interface except for the password input device;

after the user password is received at the password reading program,

i) said locks are released,

ii) the generator module is applied to the program-specific identifier H(E) and the password p to generate a program-password specific identifier, and

iii) the generated program-password specific identifier is then sent from the password reading program to the password request program, and forwarded thereby to the commercial entity to verify that the generated program-password specific identifier is the same as said pre-stored transformed password F [H(E),p];

wherein the program-specific identifier (H(E)) is derived by applying a first cryptographic function (H) to at least part of the code of the password program request, and the generated program-password-specific identifier is generated by applying a second cryptographic function (F) to the program-specific identifier (H(E)) and at least

PAGE 8/11 * RCVD AT 7/26/2005 2:26:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:5167424366 * DURATION (mm-ss):02-40

part of the received password (p), said first cryptographic function (H) and said second cryptographic function (F) each comprising a hash function.

16. (Previously Presented) A computer system according to Claim 15, wherein only the TCB and the password reading program can control the indicator means, and said indicator means is a light emitting diode.

PAGE 9/11 * RCVD AT 7/26/2005 2:26:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:5167424366 * DURATION (mm-ss):02-40